


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

 [Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE Xplore Guide](#) [e-mail](#)

Results for "((tate pairing )&lt;in&gt;metadata)"

Your search matched 12 of 1457175 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance in Descending order**.» [Search Options](#)[View Session History](#)[New Search](#)» [Key](#)

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[Modify Search](#)

((tate pairing)&lt;in&gt;metadata)

 Check to search only within this results setDisplay Format:  Citation  Citation & Abstract  1. **Performance evaluation of efficient algorithms for Tate pairing**

Matsuda, S.; Inomata, A.; Okamoto, T.; Okamoto, E.;  
*Communications, Computers and signal Processing, 2005. PACRIM. 2005 IEEE Conference on*  
 24-26 Aug. 2005 Page(s):657 - 660  
 Digital Object Identifier 10.1109/PACRIM.2005.1517375

[AbstractPlus](#) | Full Text: [PDF\(190 KB\)](#) [IEEE CNF Rights and Permissions](#)

2. **Software implementation of Tate pairing over GF(2<sup>m</sup>)**

Bertoni, G.; Breveglieri, L.; Fragneto, P.; Pelosi, G.; Sportiello, L.;  
*Design, Automation and Test in Europe, 2006. DATE '06. Proceedings Volume 2*, 6-10 March 2006 Page(s):5 pp.

[AbstractPlus](#) | Full Text: [PDF\(136 KB\)](#) [IEEE CNF Rights and Permissions](#)

3. **Parallel Hardware Architectures for the Cryptographic Tate Pairing**

Bertoni, G.; Breveglieri, L.; Fragneto, P.; Pelosi, G.;  
*Information Technology: New Generations, 2006. ITNG 2006. Third International*  
 10-12 April 2006 Page(s):186 - 191  
 Digital Object Identifier 10.1109/ITNG.2006.107

[AbstractPlus](#) | Full Text: [PDF\(208 KB\)](#) [IEEE CNF Rights and Permissions](#)

4. **The Tate pairing and the discrete logarithm applied to elliptic curve crypt**

Frey, G.; Muller, M.; Ruck, H.-G.;  
*Information Theory, IEEE Transactions on*  
 Volume 45, Issue 5, July 1999 Page(s):1717 - 1719  
 Digital Object Identifier 10.1109/18.771254

[AbstractPlus](#) | [References](#) | Full Text: [PDF\(124 KB\)](#) [IEEE JNL Rights and Permissions](#)

5. **Hardware and software normal basis arithmetic for pairing-based crypto characteristic three**

Granger, R.; Page, D.; Stam, M.;  
*Computers, IEEE Transactions on*  
 Volume 54, Issue 7, July 2005 Page(s):852 - 860  
 Digital Object Identifier 10.1109/TC.2005.120

[AbstractPlus](#) | Full Text: [PDF\(616 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

- 6. The Eta Pairing Revisited**  
Hess, F.; Smart, N.P.; Vercauteren, F.;  
[Information Theory, IEEE Transactions on](#)  
Volume 52, Issue 10, Oct. 2006 Page(s):4595 - 4602  
Digital Object Identifier 10.1109/TIT.2006.881709  
[AbstractPlus](#) | Full Text: [PDF\(312 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- 7. FPGA implementation of a GF( $2^{15}$ ) multiplier for use in pairing based cryptosystems**  
Keller, M.; Kerins, T.; Marnane, W.;  
[Field Programmable Logic and Applications, 2005. International Conference on](#)  
24-26 Aug. 2005 Page(s):594 - 597  
Digital Object Identifier 10.1109/FPL.2005.1515793  
[AbstractPlus](#) | Full Text: [PDF\(197 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- 8. A Fault Attack on Pairing-Based Cryptography**  
Page, D.; Vercauteren, F.;  
[Computers, IEEE Transactions on](#)  
Volume 55, Issue 9, Sept. 2006 Page(s):1075 - 1080  
Digital Object Identifier 10.1109/TC.2006.134  
[AbstractPlus](#) | Full Text: [PDF\(152 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- 9. FPGA acceleration of the Tate pairing in characteristic 2**  
Ronan, R.; O'Heigeartaigh, C.; Murphy, C.; Scott, M.; Kerins, T.;  
[Field Programmable Technology, 2006. FPT 2006. IEEE International Conference on](#)  
Dec. 2006 Page(s):213 - 220  
Digital Object Identifier 10.1109/FPT.2006.270314  
[AbstractPlus](#) | Full Text: [PDF\(204 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- 10. FPGA accelerated Tate pairing based cryptosystems over binary fields**  
Chang Shu; Soonhak Kwon; Kris Gaj;  
[Field Programmable Technology, 2006. FPT 2006. IEEE International Conference on](#)  
Dec. 2006 Page(s):173 - 180  
Digital Object Identifier 10.1109/FPT.2006.270309  
[AbstractPlus](#) | Full Text: [PDF\(306 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- 11. Faster identity based encryption**  
Scott, M.;  
[Electronics Letters](#)  
Volume 40, Issue 14, 8 July 2004 Page(s):861 - 862  
Digital Object Identifier 10.1049/el:20045081  
[AbstractPlus](#) | Full Text: [PDF\(192 KB\)](#) IEE JNL
- 12. Identity based authenticated key agreement protocols from pairings**  
Chen, L.; Kudla, C.;  
[Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE](#)  
30 June-2 July 2003 Page(s):219 - 233  
[AbstractPlus](#) | Full Text: [PDF\(1225 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

[Help](#) [Contact Us](#) [Privacy & Terms](#)

© Copyright 2006 IEEE -

